IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

| | |
|---|---|
| Inventor: | **: Yoshihiro ODA** |
| Filed | **: Concurrently herewith** |
| For | **: AUTHENTICATION METHOD AND....** |
| Serial No. | **: Concurrently herewith** |

July 30, 2003

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

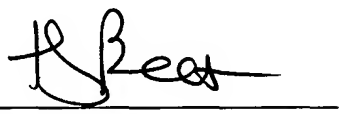
**PRIORITY CLAIM AND**

**SUBMISSION OF PRIORITY DOCUMENT**

S I R:

Applicant hereby claims priority under 35 USC 119 from **Japanese** patent application number **2002-243577** filed **August 23, 2002,** a copy of which is enclosed.

Respectfully submitted,



Thomas J. Bean
Reg. No. 44,528

Katten Muchin Zavis Rosenman
575 Madison Avenue
New York, NY 10022-2585
(212) 940-8800
Docket No.: FUJI 20.527

# 日　本　国　特　許　庁
## JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００２年　８月２３日

出願番号
Application Number: 特願２００２－２４３５７７

[ST.10/C]: [ＪＰ２００２－２４３５７７]

出願人
Applicant(s): 富士通株式会社

２００３年　１月１７日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号　出証特２００２－３１０７０６７

【書類名】　特許願
【整理番号】　0251039
【提出日】　平成14年 8月23日
【あて先】　特許庁長官　太田　信一郎　殿
【国際特許分類】　G06F 15/00
【発明の名称】　認証方法及びその装置
【請求項の数】　5
【発明者】
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
【氏名】　小田　美博
【特許出願人】
【識別番号】　000005223
【氏名又は名称】　富士通株式会社
【代理人】
【識別番号】　100070150
【住所又は居所】　東京都渋谷区恵比寿４丁目２０番３号　恵比寿ガーデンプレイスタワー３２階
【弁理士】
【氏名又は名称】　伊東　忠彦
【電話番号】　03-5424-2511
【手数料の表示】
【予納台帳番号】　002989
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　0114942

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　認証方法及びその装置

【特許請求の範囲】

【請求項１】　複数のＷｅｂサーバで特定の利用者グループにアクセスを制限するための認証方法において、

クライアント端末から前記特定の利用者グループにアクセスを限定した自装置のアクセス制限領域へのアクセス要求を受けた認証情報を持たない第１Ｗｅｂサーバは、前記特定の利用者グループにアクセスを限定したアクセス制限領域を持ち認証情報を登録した第２Ｗｅｂサーバに対し認証依頼を行い、

前記第２Ｗｅｂサーバからの認証結果を受けた前記第１Ｗｅｂサーバは、前記認証結果に応じて前記クライアント端末からの前記アクセス制限領域のアクセスを行わせることを特徴とする認証方法。

【請求項２】　請求項１記載の認証方法において、

前記第２Ｗｅｂサーバからの認証情報要求を受けた前記第１Ｗｅｂサーバは、前記認証情報要求を前記クライアント端末に渡し、

前記認証情報要求に対する前記クライアント端末からの認証情報を受けた前記第１Ｗｅｂサーバは、前記認証情報を前記第２Ｗｅｂサーバに渡すことを特徴とする認証方法。

【請求項３】　特定の利用者グループにアクセスを制限して情報提供を行うＷｅｂサーバ装置において、

前記特定の利用者グループにアクセスを制限した自装置のアクセス制限領域と同じアクセス制限領域を持ち認証情報を登録した他Ｗｅｂサーバを認証依頼先として登録した認証依頼先登録手段と、

クライアント端末からアクセスを限定したアクセス制限領域へのアクセス要求を受け、前記認証依頼先登録手段を参照して前記他Ｗｅｂサーバに対し認証依頼を行う認証依頼手段を有し、

前記第２Ｗｅｂサーバからの認証結果を受け、前記認証結果に応じて前記クライアント端末からの前記アクセス制限領域のアクセスを行わせることを特徴とするＷｅｂサーバ装置。

【請求項４】　請求項３記載の認証装置において、

前記認証依頼手段は、他Ｗｅｂサーバから受けた認証情報要求を前記クライアント端末に渡し、

前記認証情報要求に対する前記クライアント端末から受けた認証情報を前記他Ｗｅｂサーバに渡すことを特徴とする認証装置。

【請求項５】　請求項１記載の認証方法において、

前記第２Ｗｅｂサーバは、複数の第１Ｗｅｂサーバから認証依頼を行われることを特徴とする認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、認証方法及びその装置に関し、特に、複数のＷｅｂサーバで特定の利用者グループにアクセスを制限するための認証方法及びその装置に関する。

【０００２】

【従来の技術】

Ｗｅｂサーバによる情報利用が進むにつれ、ホームページによる情報提供を特定の利用者グループに限定し、複数のＷｅｂサーバで特定の利用者グループに情報提供を行いたいという要求が急増している。

【０００３】

複数のＷｅｂサーバに独立に登録され運用管理されるホームページに対して、特定の利用者グループにアクセスを限定した運用を行なうためには、各々のＷｅｂサーバが同じ認証機能を所有している必要がある。

【０００４】

ＩＤ（識別番号）とパスワードによる利用者の認証は、現在、Ｗｅｂサーバでは最もよく用いられている認証手段であるが、これを複数のＷｅｂサーバで同じように利用するためには、アクセス制限を適用する全てのＷｅｂサーバに同じ利用者のＩＤとパスワードのセットを登録しておく必要がある。または、固有のツールやシステムを使って利用者のＩＤとパスワードを共同利用する特別な仕組みが必要である。

【０００５】

ＩＤとパスワードを使用して複数のＷｅｂサーバ上に特定の利用者グループからのアクセスのみを許可するホームページを掲載し運用する場合には、これまで次のような方法が取られて来た。

【０００６】

第１の方法は、利用者が全てのＷｅｂサーバに認証情報（ＩＤとパスワード）を登録する。

【０００７】

第２の方法は、利用者はひとつのＷｅｂサーバに自分の認証情報を登録し、他Ｗｅｂサーバでは固有のツールやサーバ管理者によりコピーされた認証情報を使用する。

【０００８】

第３の方法は、Ｗｅｂサーバを置くサーバシステム間で固有のツールやシステムを使って、各Ｗｅｂサーバに登録された利用者の認証情報を相互利用する。

【０００９】

第４の方法は、利用者の認証情報を独立したサーバシステムに登録する。各Ｗｅｂサーバがこのサーバシステム固有のツールを使い、利用者の認証情報を利用する。

【００１０】

【発明が解決しようとする課題】

従来の技術を使って、特定の利用者グループにアクセスを限定するホームページを独立した複数のＷｅｂサーバで運用していくためには、次のような問題がある。

【００１１】

第１の方法で、各Ｗｅｂサーバ上に利用者が認証情報（ＩＤとパスワード）を登録する場合、利用者は複数のＷｅｂサーバで個々に登録操作を行う必要がある。利用者がＩＤやパスワードの登録を間違えたり、忘れるといったことが起こり易い。また、各Ｗｅｂサーバの管理者が個別に認証情報の管理を行う必要があり運用負荷が高くなるという問題があった。

【００１２】

第２の方法で、１つのＷｅｂサーバに全利用者の認証情報を登録し、これを他のＷｅｂサーバ上にそのままコピーして使用する場合、確実にコピーを行なうためにサーバ管理者側の操作、あるいは個別のツールが必要となる。また、全てのＷｅｂサーバ上の認証情報を時間遅れ無しでタイムリーに更新する仕組みは運用が難しいという問題があった。

【００１３】

第３の方法で、Ｗｅｂサーバを置くサーバシステム間で互いに認証情報の共有する場合、各サーバ間で認証情報を共有するために固有のシステムが必要となる。また、この場合、各サーバ間の相互連携はシステムの運用を複雑にし、運用管面の負荷を増大させるという問題があった。

【００１４】

第４の方法で、利用者の認証情報を独立したサーバシステムで一括登録管理し、これを各Ｗｅｂサーバで利用する場合、各々のＷｅｂサーバではこの独立したサーバシステムにアクセスするための固有のツールや機能が必要となる。例えばディレクトリサーバを使い認証情報を集中登録管理する場合には、ホームページのアクセス制限で使うために、さらにＷｅｂサーバのどのページをどの利用者がアクセス可能か、といったような情報も別途登録して管理する必要があり、情報の登録管理及び運用方法ともに複雑となってしまうという問題があった。

【００１５】

例えば、ＬＤＡＰ（Ｌｉｇｈｔｗｅｉｇｈｔ　Ｄｉｒｅｃｔｏｒｙ　Ａｃｃｅｓｓ　Ｐｒｏｔｏｃｏｌ）を使ってディレクトリサーバに登録された利用者の情報を各Ｗｅｂサーバから利用する場合、ディレクトリサーバには認証情報やＷｅｂサーバでアクセス制限を適用する領域やパターンに関する情報を登録しておかねばならない。

【００１６】

本発明は、上記の点に鑑みなされたものであり、複数のＷｅｂサーバで特定の利用者グループにアクセスを制限するために、利用者の手間を低減でき、Ｗｅｂサーバの運用管理の負担を少なくできる認証方法及びその装置を提供することを

目的とする。

【００１７】

【課題を解決するための手段】

請求項１，３に記載の発明は、クライアント端末から特定の利用者グループにアクセスを限定した自装置のアクセス制限領域へのアクセス要求を受けた認証情報を持たない第１Ｗｅｂサーバは、特定の利用者グループにアクセスを限定したアクセス制限領域を持ち認証情報を登録した第２Ｗｅｂサーバに対し認証依頼を行い、第２Ｗｅｂサーバからの認証結果を受けた第１Ｗｅｂサーバは、認証結果に応じてクライアント端末からのアクセス制限領域のアクセスを行わせることにより、

複数のＷｅｂサーバで特定の利用者グループにアクセスを制限するための利用者の手間を低減でき、Ｗｅｂサーバの運用管理の負担を少なくすることが可能となる。

【００１８】

請求項２，４に記載の発明は、第２Ｗｅｂサーバからの認証情報要求を受けた第１Ｗｅｂサーバは、認証情報要求をクライアント端末に渡し、認証情報要求に対するクライアント端末からの認証情報を受けた第１Ｗｅｂサーバは、認証情報を前記第２Ｗｅｂサーバに渡すことにより、請求項１の発明を実現することが可能となる。

【００１９】

請求項５に記載の発明では、第２Ｗｅｂサーバは、複数の第１Ｗｅｂサーバから認証依頼を行われることにより、一つの第２Ｗｅｂサーバで複数の第１Ｗｅｂサーバから依頼された認証を行うことができる。

【００２０】

付記６に記載の発明では、第１Ｗｅｂサーバは、複数の第２Ｗｅｂサーバに対し認証依頼を行うことにより、利用者グループごとに異なる第２Ｗｅｂサーバで認証を行うことが可能となる。

【００２１】

付記７に記載の発明では、第１Ｗｅｂサーバは、他の第１Ｗｅｂサーバに対し

認証依頼を行い、他の第１Ｗｅｂサーバから第２Ｗｅｂサーバに対し認証依頼を行うことにより、複数の第１Ｗｅｂサーバを経て最後にたどり着く第２Ｗｅｂサーバで認証を行うことが可能となる。

【００２２】

【発明の実施の形態】

図１は、本発明の原理図を示す。同図中、認証依頼Ｗｅｂサーバ１０は、本発明の機能を有するＷｅｂサーバであり、制御部１２とページデータ部１４とを有している。制御部１２には、認証依頼機能１３が設けられている。また、ページデータ部１４には、認証依頼先ＵＲＬ定義領域１５及びグループＵのみアクセス可能なアクセス制限領域１６が設けられている。

【００２３】

クライアント端末２０のＷｅｂブラウザ２２からは、利用者が認証依頼Ｗｅｂサーバ１０にあるアクセス制限が適用されたホームページに対するアクセス要求が行われる。

【００２４】

マスターＷｅｂサーバ３０は、通常のＷｅｂサーバを指すが、本明細書では特に認証依頼Ｗｅｂサーバ１０と区別するためにこの名称を使用しており、マスターＷｅｂサーバ３０とは、利用者が認証のために入力した認証情報（ＩＤとパスワード）を既にユーザ登録簿３５に登録済の認証情報と照合することにより、認証判定処理を行なうＷｅｂサーバを指す。マスターＷｅｂサーバ３０は、制御部３２とページデータ部３４とを有している。制御部３２には、認証判定処理を行なう認証機能３３が設けられている。ページデータ部３４には、ユーザ登録簿３５と共に、グループＵのみアクセス可能なアクセス制限領域３６が設けられている。

【００２５】

認証依頼Ｗｅｂサーバ１０は、通常のＷｅｂサーバであるマスターＷｅｂサーバ３０が持つ機能に加えて、さらに次の２つの機能を持つ。第１の機能は、認証依頼先ＵＲＬ定義領域１５であり、アクセス制限を適用する自Ｗｅｂサーバ上のアクセス制限領域１６に対応させて設けている。認証依頼先ＵＲＬ定義領域１５

には自Ｗｅｂサーバ上で適用したいアクセス制限と同じアクセス制限を使用している他Ｗｅｂサーバのアクセス制限領域（例えばマスターＷｅｂサーバ３０のアクセス制限領域３６）を参照するためのＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｃｅ　Ｌｏｃａｔｏｒ）が登録されている。

【００２６】

第２の機能は、認証依頼先ＵＲＬ定義領域１５から読み出された該当の他ＷｅｂサーバのＵＲＬにアクセスすることで認証の可否を確認する認証依頼機能１３である。認証依頼機能１３は、自Ｗｅｂサーバ上の当該アクセス制限下にあるアクセス制限領域１６のホームページに利用者がアクセスした場合、利用者が入力するＩＤとパスワードを使って他サーバ（例えばマスターＷｅｂサーバ３０）にアクセスし、その認証の可否を決定する機能を持つ。

【００２７】

以上の２つの機能により、自Ｗｅｂサーバ上に直接、利用者の認証情報を持っていない場合でも、他Ｗｅｂサーバの認証機能を使うことで、自Ｗｅｂサーバにアクセス制限を適用したホームページを提供できる。

【００２８】

なお、認証依頼Ｗｅｂサーバ１０は、通常のＷｅｂサーバであるマスターＷｅｂサーバ３０が持つ機能も持っているため、自Ｗｅｂサーバ上のアクセス制限されていない領域のホームページに利用者がアクセスした場合は、この領域からアクセスされたホームページを読み出した利用者に提供する。

【００２９】

図２を用いて利用者が自分の属するグループＵのみアクセスを許可されているアクセス制限領域１６内のページ（ｄａｔａ．ｈｔｍｌ）の取得を要求した場合の処理の流れを説明する。

【００３０】

ここで、利用者の認証情報はマスターＷｅｂサーバ３０のユーザ登録簿３５にのみ登録されており、認証依頼Ｗｅｂサーバ１０には存在しない。マスターＷｅｂサーバ３０でグループＵのみアクセスを許可されているアクセス制限領域３６内のページのひとつを“／ｓｅｃｒｉｔ／ｃｈｅｃｋ．ｈｔｍｌ”とする。

【００３１】

認証依頼Ｗｅｂサーバ１０には、このページのＵＲＬ“ＡＡＡ．ｃｏｍ／／ｓｅｃｒｉｔ／ｃｈｅｃｋ．ｈｔｍ”が、グループUのみアクセスを許可されているアクセス制限領域１６と対応させて、認証依頼先ＵＲＬ定義領域１５に登録されている。

【００３２】

認証依頼機能１３は利用者から要求されたページの属するアクセス制限領域１６に対応して認証依頼先ＵＲＬ定義領域１５が存在する場合には、自Ｗｅｂサーバでの認証処理を行なわずに、認証依頼先ＵＲＬ定義領域１５で指定されたＵＲＬ“ＡＡＡ．ｃｏｍ／／ｓｅｃｒｉｔ／ｃｈｅｃｋ．ｈｔｍ”のアクセスによりマスターＷｅｂサーバ３０を利用した認証処理を行なう。

【００３３】

①クライアント端末２０は、認証依頼Ｗｅｂサーバ１０上のアクセス制限領域１６にあるアクセス制限されたページ［ｄａｔａ．ｈｔｍｌ］の取得を要求する。

【００３４】

②認証依頼Ｗｅｂサーバ１０の認証依頼機能１３は、要求されたページがあるアクセス制限領域１６に対応した認証依頼先ＵＲＬ定義領域１５が存在するか否かを調べ、存在する場合には認証依頼先ＵＲＬ定義領域１５から読み出したＵＲＬ“ＡＡＡ．ｃｏｍ／／ｓｅｃｒｉｔ／ｃｈｅｃｋ．ｈｔｍ”にアクセスする。ここでは、ＨＴＴＰプロトコルでのページ要求、あるいはページ更新チェックなどのコマンドを用いる。

【００３５】

③マスターＷｅｂサーバ３０は、アクセス制限領域３６にあるＵＲＬ“ＡＡＡ．ｃｏｍ／／ｓｅｃｒｉｔ／ｃｈｅｃｋ．ｈｔｍ”のアクセスなので認証依頼Ｗｅｂサーバ１０の認証依頼機能１３に対してＩＤとパスワードを要求する。

【００３６】

④認証依頼Ｗｅｂサーバ１０は、利用者に対してマスターＷｅｂサーバから要求された形式のＩＤとパスワードの入力を要求する。

【００３７】

⑤利用者は、ＷＥＢブラウザ２２から要求されたＩＤとパスワードを入力する。

【００３８】

⑥認証依頼機能１３は、ＷＥＢブラウザ２２から供給される上記ＩＤとパスワードをマスターＷｅｂサーバ３０に返す。

【００３９】

⑦認証機能３３は、認証ＯＫの場合その旨の応答を認証依頼Ｗｅｂサーバ１０に返す。

【００４０】

⑧認証依頼Ｗｅｂサーバ１０は認証ＯＫの応答により、利用者に最初に要求されたｄａｔａ．ｈｔｍｌをアクセス制限領域１６から読み出し、ＷＥＢブラウザ２２に渡す。

【００４１】

図３に、認証依頼機能１３での制御の流れを自サーバで認証処理を行う場合の制御の流れと対比させて示す。同図中、アクセス制限を適用したページの取得要求があると、実線の矢印で示すように、認証依頼機能１３はステップＳ１０で要求ページに該当するマスターＷｅｂサーバ３０のＵＲＬにアクセスする。そして、マスターＷｅｂサーバ３０からＩＤとパスワードの要求を受けると、ステップＳ１２でこの要求をＷＥＢブラウザ２２に渡す。ＷＥＢブラウザ２２からＩＤとパスワードが供給されると、ステップＳ１４でこのＩＤとパスワードをマスターＷｅｂサーバ３０に渡し、認証ＯＫの応答を受けると要求ページをＷＥＢブラウザ２２に渡す。

【００４２】

これに対し、自サーバで認証処理を行う場合、アクセス制限を適用したページの取得要求があると、破線の矢印で示すように、自サーバはステップＳ２０でＩＤとパスワードをＷＥＢブラウザ２２に要求する。ＷＥＢブラウザ２２からＩＤとパスワードが供給されると、ステップＳ２２でこのＩＤとパスワードを自サーバ内のユーザ登録簿と照合し、認証ＯＫの場合にステップＳ２４で自サーバから

要求ページをＷＥＢブラウザ２２に渡す。

【００４３】

図４を用いて他Ｗｅｂサーバの参照処理を再帰的に使用する実施例について説明する。同図中、クライアント端末２０から認証依頼Ｗｅｂサーバ１０上のアクセス制限領域１６にあるアクセス制限されたページの取得要求が行われ、認証依頼Ｗｅｂサーバ１０から認証依頼を受けたＷｅｂサーバが認証依頼Ｗｅｂサーバ４０であった場合、この認証依頼Ｗｅｂサーバ４０は次のＷｅｂサーバに認証依頼を出す。この認証依頼は一または複数の認証依頼Ｗｅｂサーバ４０を経てマスターＷｅｂサーバ３０に渡される。

【００４４】

その後、マスターＷｅｂサーバ３０からのＩＤとパスワードの要求は上記認証依頼とは逆の経路で認証依頼Ｗｅｂサーバ４０，１０を経てクライアント端末２０に渡され、これに対するクライアント端末２０の応答（ＩＤとパスワード）は認証依頼Ｗｅｂサーバ１０，４０を経てマスターＷｅｂサーバ３０に渡される。そして、マスターＷｅｂサーバ３０からの認証ＯＫの応答が認証依頼Ｗｅｂサーバ４０から認証依頼Ｗｅｂサーバ１０に渡され、認証依頼Ｗｅｂサーバ１０は要求ページをクライアント端末２０に渡す。

【００４５】

このように経路内に複数の認証依頼Ｗｅｂサーバ１０，４０がある場合にも、実際に利用者が入力したＩＤとパスワードを既に登録されている認証情報と照らし合わせる認証処理を行なうのは、最後にたどり着くマスタＷｅｂサーバ３０である。

【００４６】

図５（Ａ），（Ｂ），（Ｃ）に認証依頼Ｗｅｂサーバの基本的な構成パターンを示す。図５（Ａ）のパターンでは、１つのマスターＷｅｂサーバ３０を複数の認証依頼Ｗｅｂサーバ１０ａ～１０ｃからアクセスして利用する。

【００４７】

図５（Ｂ）のパターンでは、１つの認証依頼Ｗｅｂサーバ１０から複数のマスタＷｅｂサーバ３０ａ～３０ｃを参照する。この場合、認証依頼Ｗｅｂサーバ１

０上に、それぞれ異なるアクセス制限を適用するアクセス制限領域１６ａ，１６ｂ，１６ｃ各々に対して認証依頼先ＵＲＬ定義領域１５ａ，１５ｂ，１５ｃを設け、それぞれによりマスタＷｅｂサーバ３０ａ～３０ｃを参照する。

【００４８】

図５（Ｃ）のパターンでは、認証依頼Ｗｅｂサーバ１０が認証を依頼するＷｅｂサーバが認証依頼Ｗｅｂサーバ４０であり、認証依頼Ｗｅｂサーバ４０からマスタＷｅｂサーバ２０に認証を依頼する。図４と同一構成であり、認証依頼Ｗｅｂサーバ４０が複数段従属接続されてもよい。

【００４９】

図６は、本発明の第１実施例のシステム構成図を示す。このシステムは会社内に構築される。本社のＷｅｂサーバ５０がマスターＷｅｂサーバとされ、このＷｅｂサーバ５０上には経理関係者のみがアクセス可能なアクセス制限領域５６が定義されると共に、本社と支社を含む会社の全経理関係者のＩＤとパスワードを登録したユーザ登録簿５５が設けられている。

【００５０】

各支店のＷｅｂサーバ６０，７０は認証依頼Ｗｅｂサーバとして構成されており、各支店で作成登録した経理関係者のみにアクセスを限定するホームページの開設は、本社のＷｅｂサーバ５０のアクセス制限領域５６を参照することで可能となる。各支店のＷｅｂサーバ６０，７０それぞれで個別に認証のためのＩＤとパスワードの登録は必要がない。

【００５１】

本社Ｗｅｂサーバ５０のアクセス制限領域５６に属する任意のＵＲＬが公開されていれば、各支店ではこれを支店のＷｅｂサーバに登録するだけで、本社のＷｅｂサーバで実施しているのと同一のアクセス制限条件下（経理関係者のＩＤとパスワード）でアクセス制限領域６６，７６にてホームページを提供することが可能となる。

【００５２】

経理関係者はクライアント端末８０からＩＤとパスワードを入力することにより、Ｗｅｂサーバ５０，６０，７０それぞれのアクセス制限領域５６，６６，７

６のホームページをアクセスすることができる。

【００５３】

図７は、本発明の第２実施例のシステム構成図を示す。このシステムは公共施設のＷｅｂサーバで実施される。市役所のＷｅｂサーバ８０では各種団体やグループが自分達のホームページを開設することを認めており、このＷｅｂサーバ８０を認証依頼Ｗｅｂサーバで構成する。

【００５４】

そして、政党本部Ｗｅｂサーバ９０、県庁Ｗｅｂサーバ１００、趣味の会Ｗｅｂサーバ１１０それぞれをマスターＷｅｂサーバで構成し、各Ｗｅｂサーバ９０，１００，１１０それぞれに、政党関係者全員のＩＤとパスワードを登録したユーザ登録簿９５、県職員全員のＩＤとパスワードを登録したユーザ登録簿１０５、趣味の会の会員全員のＩＤとパスワードを登録したユーザ登録簿１１５を設ける。

【００５５】

市役所のＷｅｂサーバ８０には、各種団体やグループそれぞれだけがアクセス可能なアクセス制限領域８６ａ，８６ｂ，８６ｃとこれに対応する認証依頼先ＵＲＬ定義領域を定義し、アクセス制限領域８６ａ，８６ｂ，８６ｃそれぞれに各グループのホームページを設ける。

【００５６】

これにより、各種団体やグループそれぞれは、クライアント端末１２０，１２２から市役所のＷｅｂサーバ８０に接続し、Ｗｅｂサーバ８０から各々のマスターＷｅｂサーバであるＷｅｂサーバ９０，１００，１１０の該当ＵＲＬを参照して各グループのＩＤとパスワードの認証を行い、アクセスを制限したアクセス制限領域８６ａ，８６ｂ，８６ｃに設定した各グループのホームページを閲覧することができる。

【００５７】

図８に、認証依頼先ＵＲＬ定義の一実施例を示す。図８では、左側の認証依頼Ｗｅｂサーバ１０で定義する認証依頼先ＵＲＬ定義ファイル“．ｈｔａｃｃｅｓｓ＿Ｅ”を、右側のＵＮＩＸ（登録商標）で動作する従来のＷｅｂサーバで使用

されているアクセス制限定義ファイル“．ｈｔａｃｃｅｓｓファイル”と比較して示している。両方ともアクセス制限を適用するアクセス制限領域の最上位のディレクトリ配下に設置して使用する。なお、図中、上段は定義形式、下段は定義例を示す。

【００５８】

認証依頼先ＵＲＬ定義ファイル“．ｈｔａｃｃｅｓｓ＿Ｅ”でのパラメタは次のように定義されている。ＡｕｔｈＵＲＬは認証処理のために参照するサーバのＵＲＬを記述する。ＡｕｔｈＮａｍｅは認証に与える名称（利用者のブラウザの表示で見せるためのものなので任意に設定できる）である。ＡｕｔｈＴｙｐｅは認証手法であり、ここでは定義しない。マスターＷｅｂサーバから指定された認証手法を使って利用者にＩＤとパスワードを要求するので、この情報は認証依頼機能で判定、設定して使用する。

【００５９】

本発明によれば、ホームページ利用者にとっては、マスターＷｅｂサーバ３０となるサーバにだけ自分のＩＤとパスワードを登録すればよく、複数のＷｅｂサーバに何度もＩＤやパスワードを入れる手間がなくなり、自分のＩＤとパスワードを忘れて困る、ということも少なくなる。

【００６０】

また、ホームページ開設者にとっては、自分達のグループにアクセスを限定したホームページを身近なＷｅｂサーバを使って開設することが容易にでき、グループ内でのホームページでの情報提供を分担して行うことが容易となる。更に、ＩＤとパスワードが一箇所での集中管理となるので、複数のサーバで登録管理する場合に比べて認証情報を運用管理する者の負担が少なくなる。

【００６１】

また、Ｗｅｂサーバ管理者にとっては、マスターＷｅｂサーバ側の管理者はこれを参照する認証依頼Ｗｅｂサーバの存在を意識する必要はない。Ｗｅｂサーバ間での認証情報交換のための特別なシステムも不要なので運用での新たな負荷は発生しない。また、連携に必要なＵＲＬ情報は公開しても差し支えない性格のものなので、広報、伝達時の情報の扱いが簡単である。更に、自Ｗｅｂサーバ上で

のＩＤとパスワード管理と併用可能なので、通常のＷｅｂサーバから認証依頼Ｗｅｂサーバに移行した場合でも従来通りの運用は全く影響を受けない。

なお、認証依頼Ｗｅｂサーバ１０が請求項記載の第１Ｗｅｂサーバに対応し、マスターＷｅｂサーバ３０が第２Ｗｅｂサーバに対応し、認証依頼先ＵＲＬ定義領域１５が認証依頼先登録手段に対応し、認証依頼機能１３が認証依頼手段に対応する。

【００６２】

（付記１）　複数のＷｅｂサーバで特定の利用者グループにアクセスを制限するための認証方法において、

クライアント端末から前記特定の利用者グループにアクセスを限定した自装置のアクセス制限領域へのアクセス要求を受けた認証情報を持たない第１Ｗｅｂサーバは、前記特定の利用者グループにアクセスを限定したアクセス制限領域を持ち認証情報を登録した第２Ｗｅｂサーバに対し認証依頼を行い、

前記第２Ｗｅｂサーバからの認証結果を受けた前記第１Ｗｅｂサーバは、前記認証結果に応じて前記クライアント端末からの前記アクセス制限領域のアクセスを行わせることを特徴とする認証方法。

【００６３】

（付記２）　付記１記載の認証方法において、

前記第２Ｗｅｂサーバからの認証情報要求を受けた前記第１Ｗｅｂサーバは、前記認証情報要求を前記クライアント端末に渡し、

前記認証情報要求に対する前記クライアント端末からの認証情報を受けた前記第１Ｗｅｂサーバは、前記認証情報を前記第２Ｗｅｂサーバに渡すことを特徴とする認証方法。

【００６４】

（付記３）　特定の利用者グループにアクセスを制限して情報提供を行うＷｅｂサーバ装置において、

前記特定の利用者グループにアクセスを制限した自装置のアクセス制限領域と同じアクセス制限領域を持ち認証情報を登録した他Ｗｅｂサーバを認証依頼先として登録した認証依頼先登録手段と、

クライアント端末からアクセスを限定したアクセス制限領域へのアクセス要求を受け、前記認証依頼先登録手段を参照して前記他Ｗｅｂサーバに対し認証依頼を行う認証依頼手段を有し、

前記第２Ｗｅｂサーバからの認証結果を受け、前記認証結果に応じて前記クライアント端末からの前記アクセス制限領域のアクセスを行わせることを特徴とするＷｅｂサーバ装置。

【００６５】

（付記４）　付記３記載の認証装置において、

前記認証依頼手段は、他Ｗｅｂサーバから受けた認証情報要求を前記クライアント端末に渡し、

前記認証情報要求に対する前記クライアント端末から受けた認証情報を前記他Ｗｅｂサーバに渡すことを特徴とする認証装置。

【００６６】

（付記５）　付記１記載の認証方法において、

前記第２Ｗｅｂサーバは、複数の第１Ｗｅｂサーバから認証依頼を行われることを特徴とする認証方法。

【００６７】

（付記６）　付記１記載の認証方法において、

前記第１Ｗｅｂサーバは、複数の第２Ｗｅｂサーバに対し認証依頼を行うことを特徴とする認証方法。

【００６８】

（付記７）　付記１記載の認証方法において、

前記第１Ｗｅｂサーバは、他の第１Ｗｅｂサーバに対し認証依頼を行い、

前記他の第１Ｗｅｂサーバから前記第２Ｗｅｂサーバに対し認証依頼を行うことを特徴とする認証方法。

【００６９】

【発明の効果】

上述の如く、請求項１，３に記載の発明によれば、複数のＷｅｂサーバで特定の利用者グループにアクセスを制限するための利用者の手間を低減でき、Ｗｅｂ

サーバの運用管理の負担を少なくすることが可能となる。

【００７０】

また、請求項２，４に記載の発明によれば、請求項１の発明を実現することが可能となる。

【００７１】

また、請求項５に記載の発明によれば、一つの第２Ｗｅｂサーバで複数の第１Ｗｅｂサーバから依頼された認証を行うことができる。

【００７２】

また、付記６に記載の発明によれば、利用者グループごとに異なる第２Ｗｅｂサーバで認証を行うことが可能となる。

【００７３】

また、付記７に記載の発明によれば、複数の第１Ｗｅｂサーバを経て最後にたどり着く第２Ｗｅｂサーバで認証を行うことが可能となる。

【図面の簡単な説明】

【図１】

本発明の原理図である。

【図２】

アクセス制限領域内のページの取得を要求した場合の処理の流れを説明するための図である。

【図３】

認証依頼機能での制御の流れを自サーバで認証処理を行う場合の制御の流れと対比させて示す図である。

【図４】

他Ｗｅｂサーバの参照処理を再帰的に使用する実施例を説明するための図である。

【図５】

認証依頼Ｗｅｂサーバの基本的な構成パターンを示す図である。

【図６】

本発明の第１実施例のシステム構成図である。

【図７】

本発明の第２実施例のシステム構成図である。

【図８】

認証依頼先ＵＲＬ定義の一実施例を示す図である。

【符号の説明】

１０　認証依頼Ｗｅｂサーバ

１２　制御部

１３　認証依頼機能

１４　ページデータ部

１５　認証依頼先ＵＲＬ定義領域

１６　アクセス制限領域

２０　クライアント端末

２２　Ｗｅｂブラウザ

３０　マスターＷｅｂサーバ

３２　制御部

３４　ページデータ部

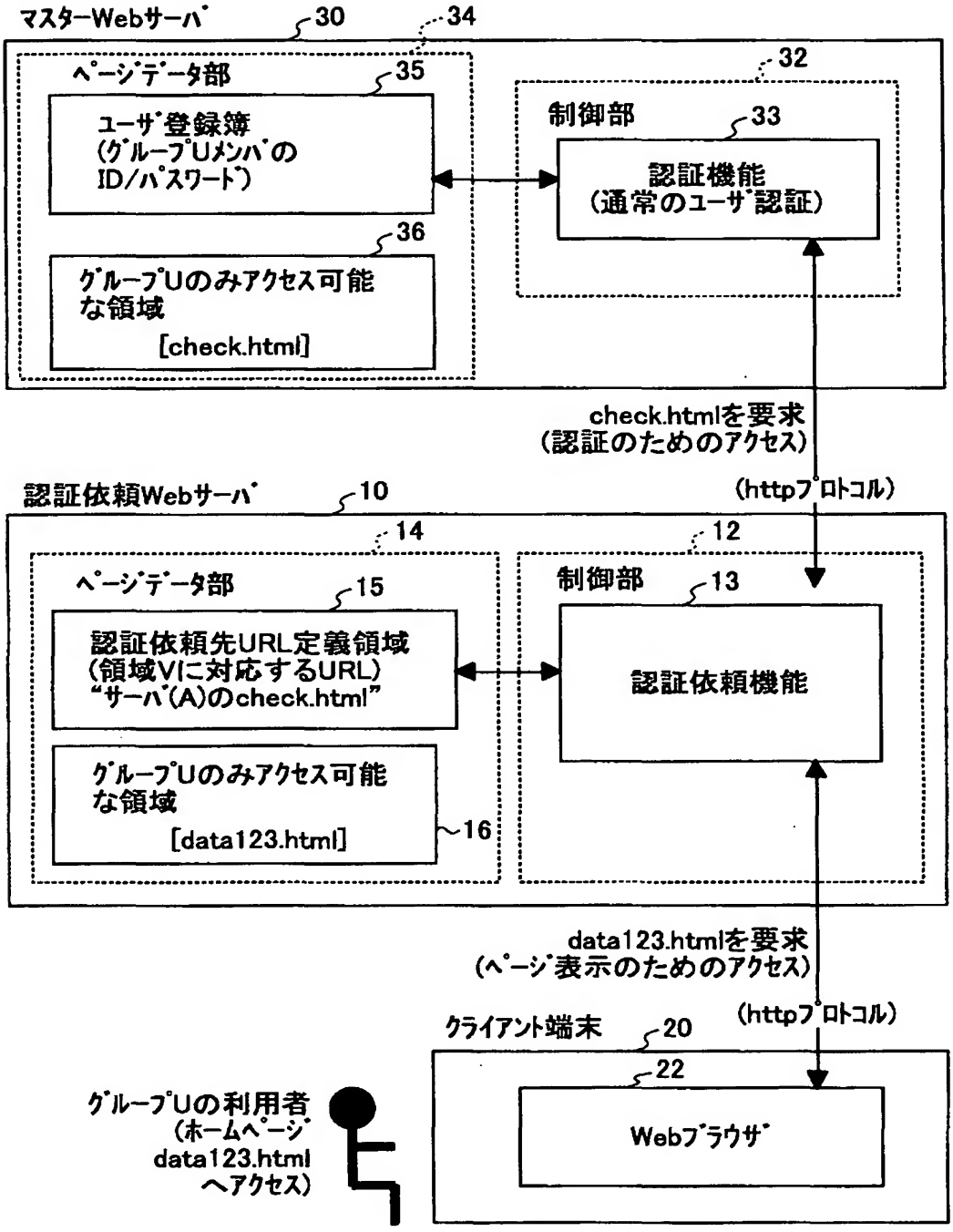
３５　ユーザ登録簿

３６　アクセス制限領域

【書類名】　　図面

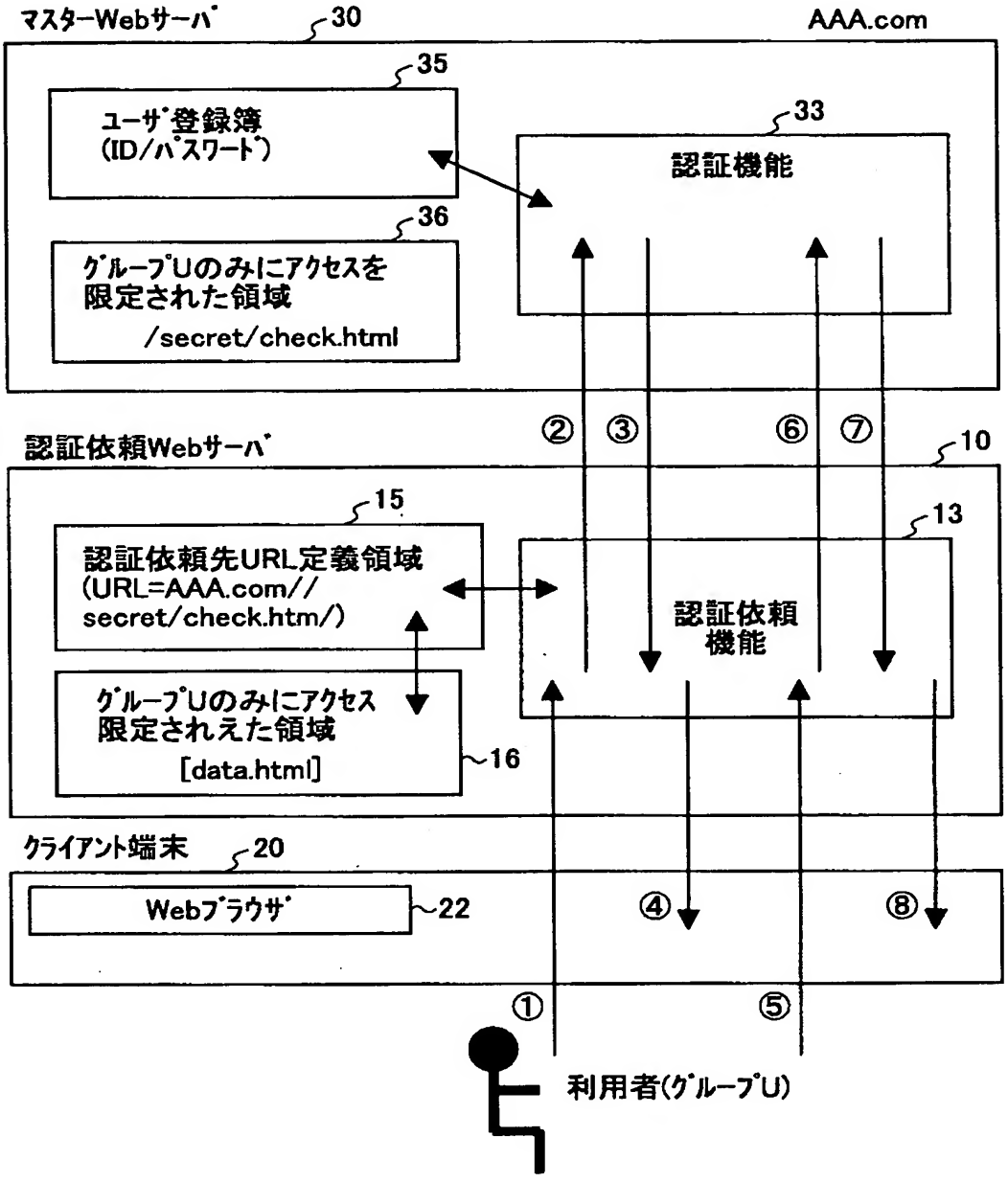
【図１】

本発明の原理図



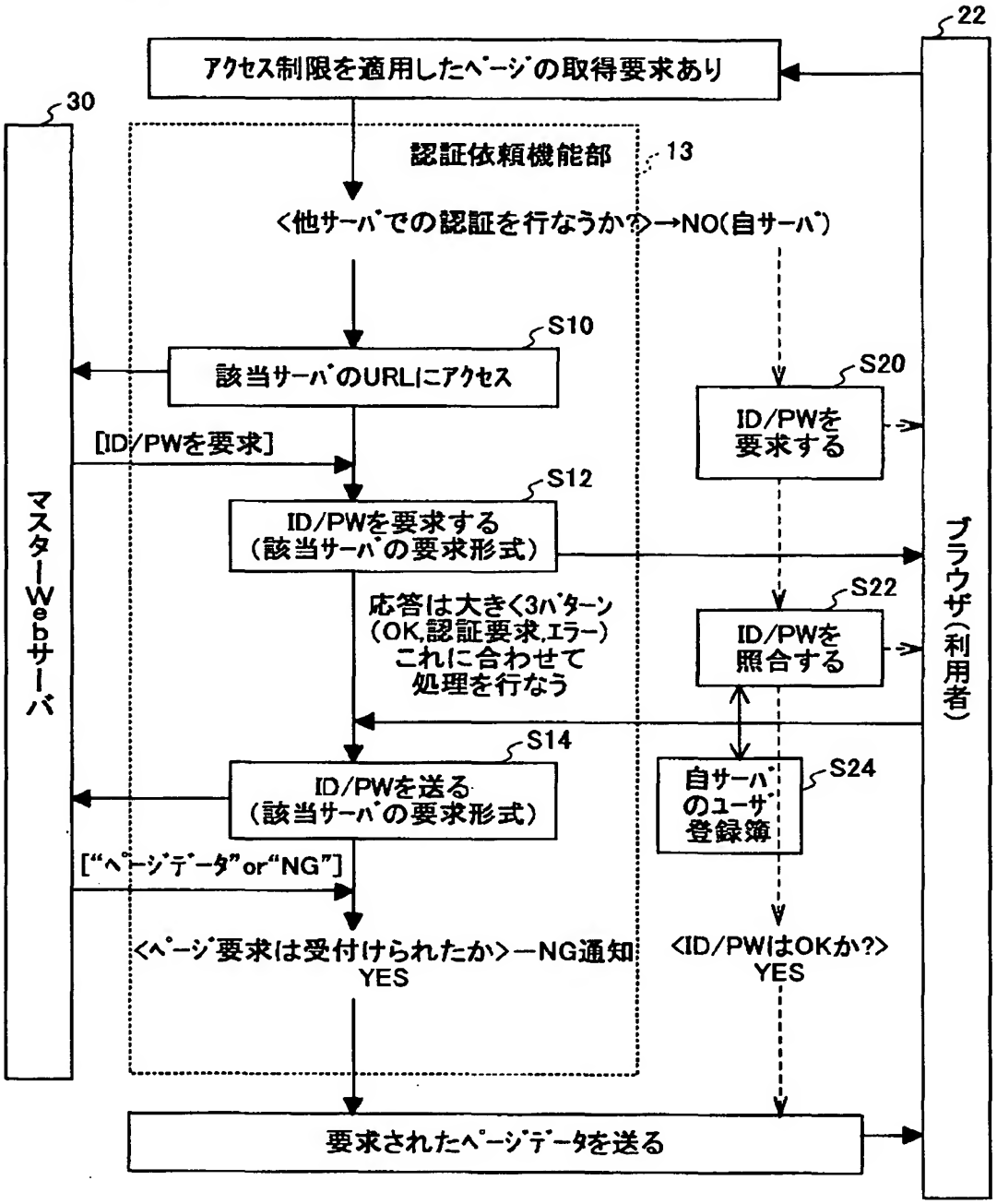
【図２】

アクセス制限領域内のページの取得を要求した場合の処理の流れを説明するための図



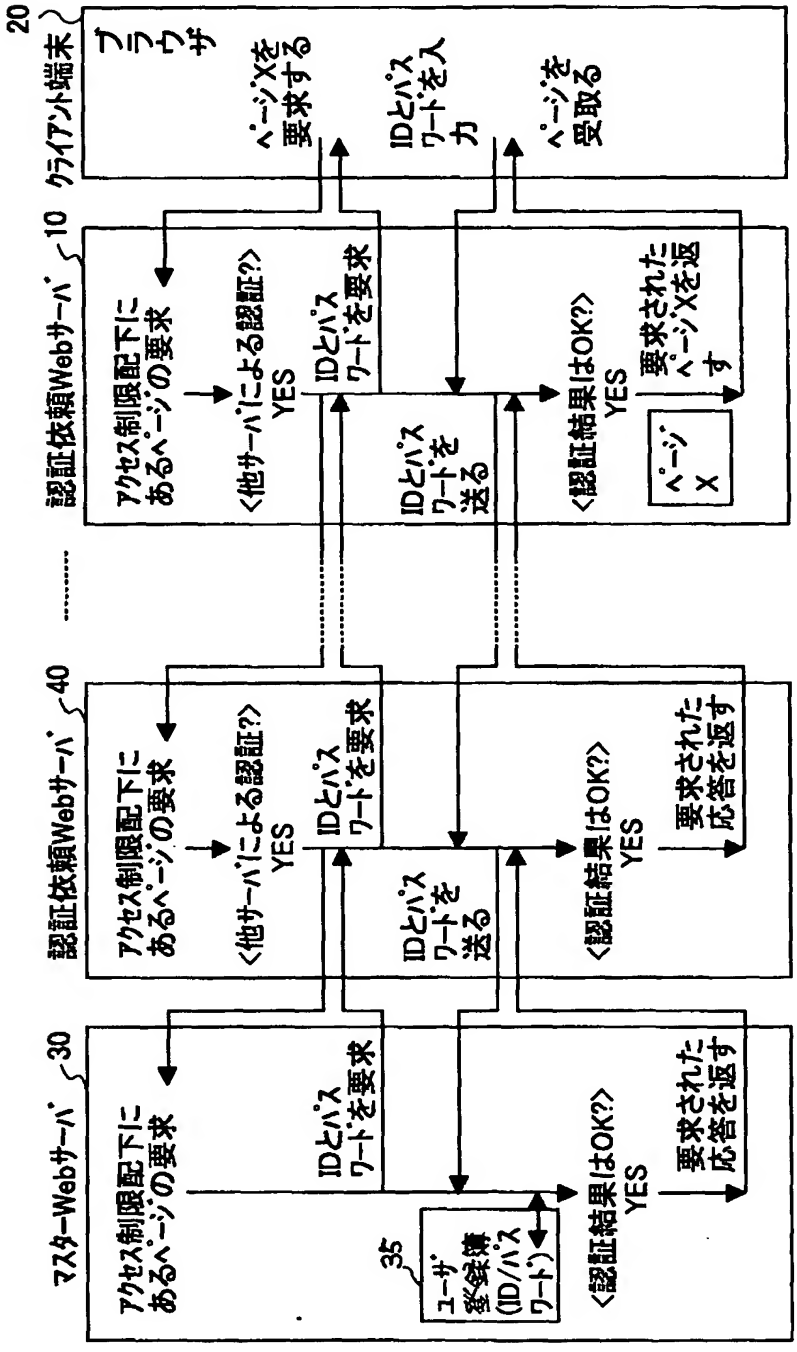
【図３】

認証依頼機能での制御の流れを自サーバで
認証処理を行う場合の流れと対比させて示す図



【図４】

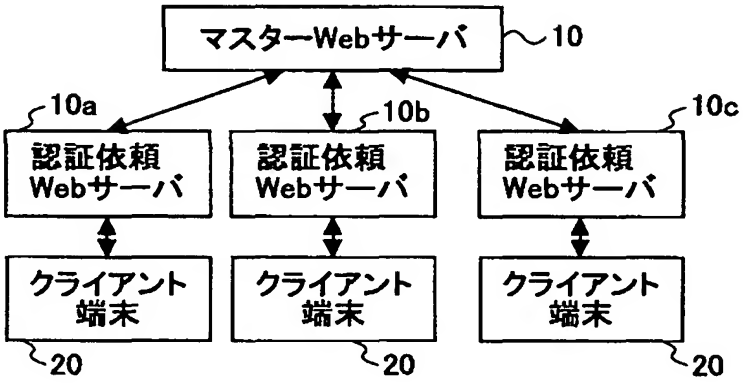
他Ｗｅｂサーバの参照処理を再帰的に使用する実施例を説明するための図



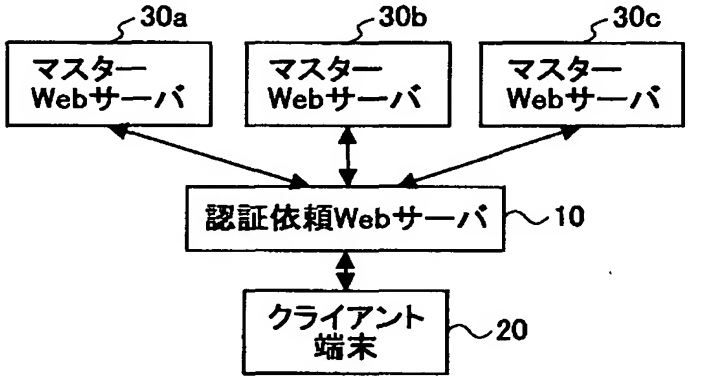
【図５】

認証依頼Ｗｅｂサーバの基本的な構成パターンを示す図

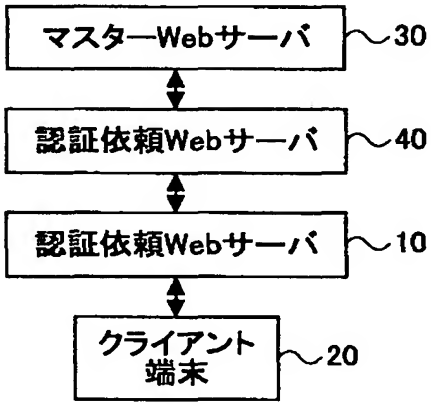
(A)




(B)

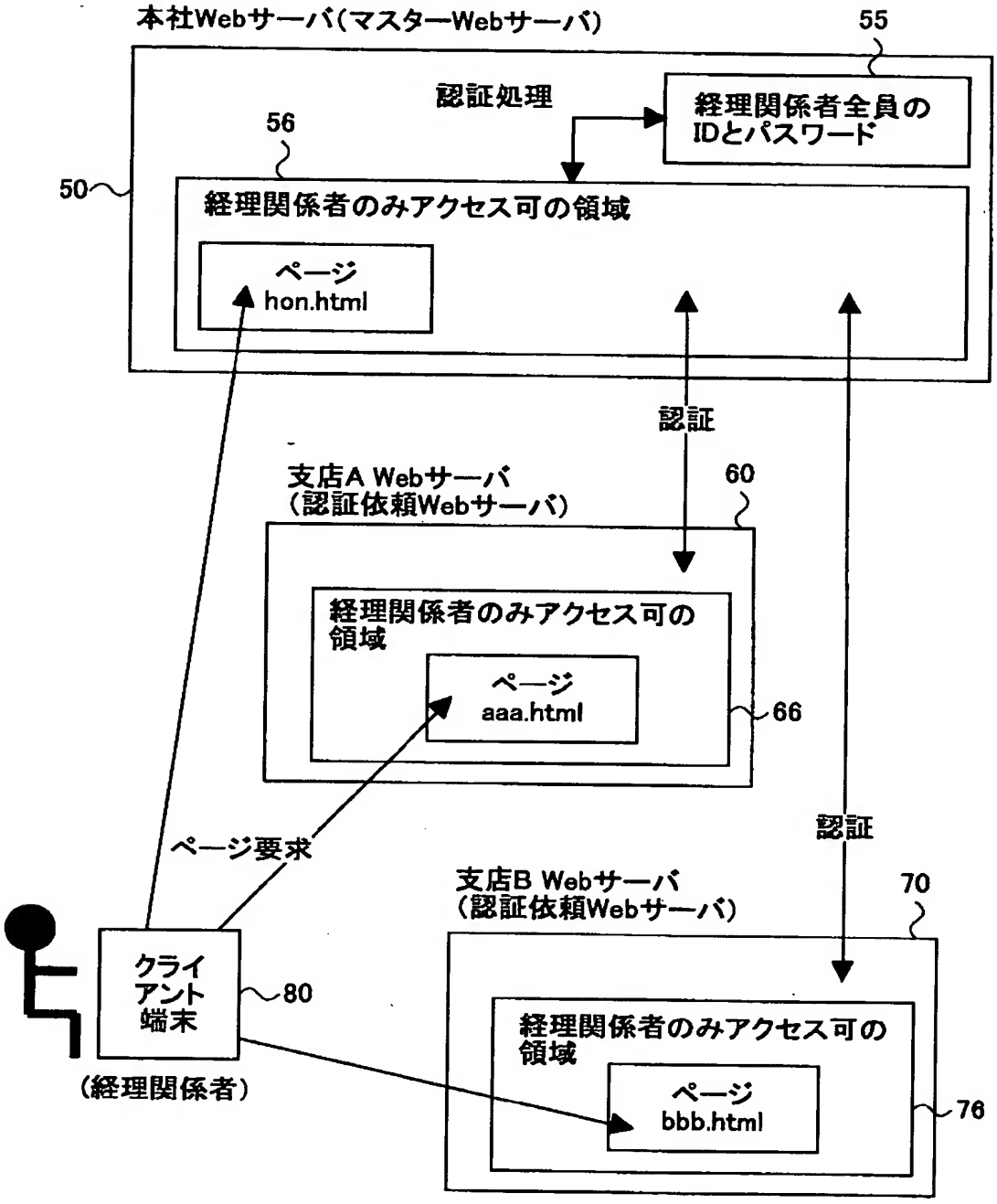



(C)



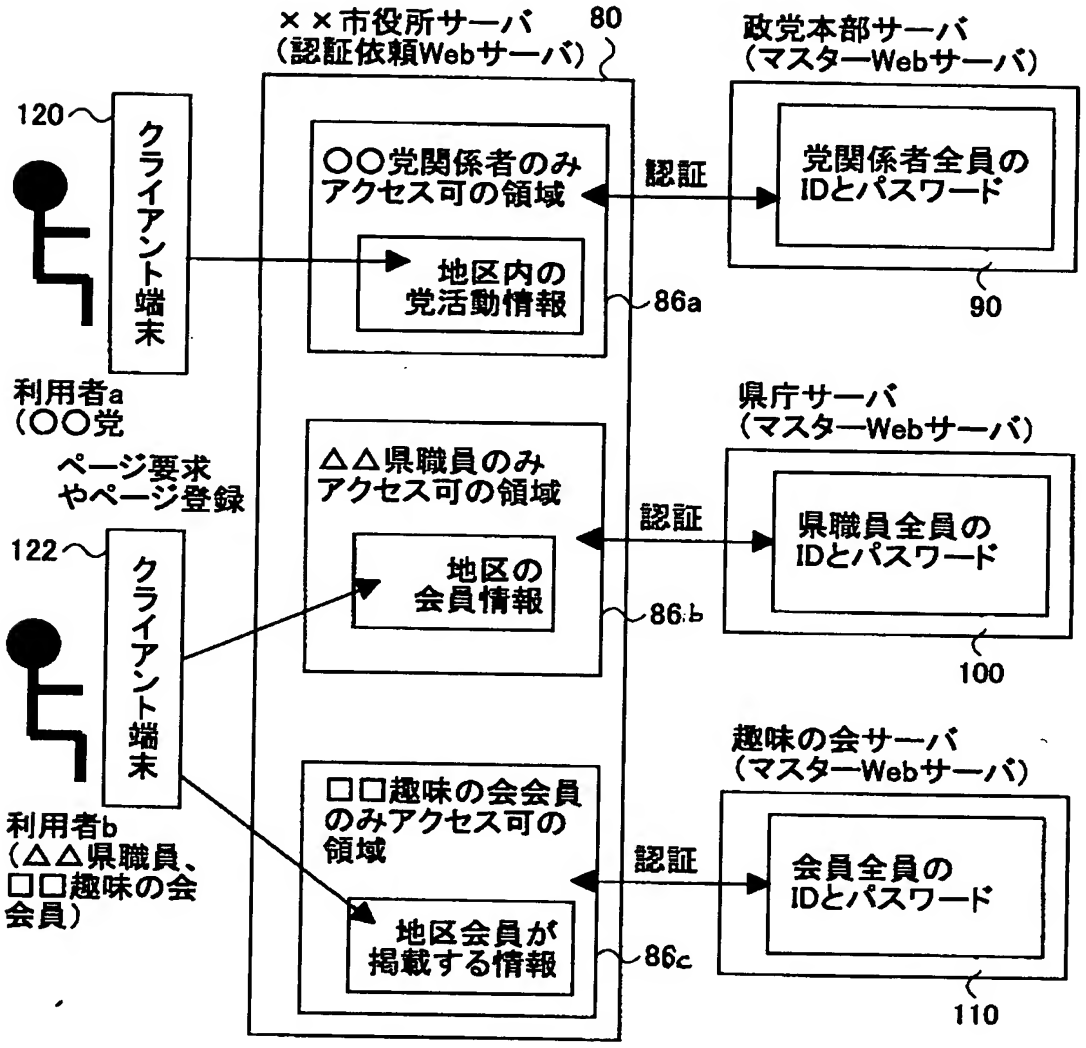
【図６】

本発明の第１実施例のシステム構成図



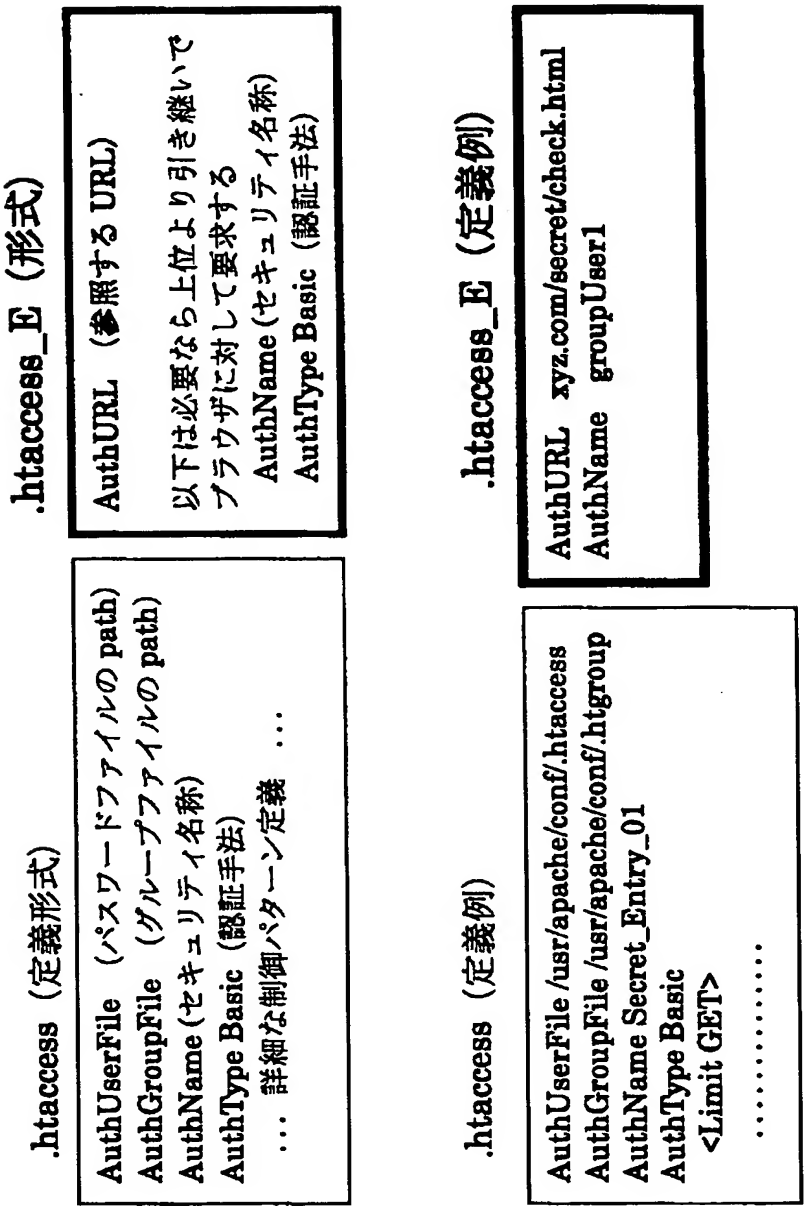
【図７】

本発明の第２実施例のシステム構成図



【図８】

認証依頼先ＵＲＬ定義の一実施例を示す図



【書類名】　　要約書

【要約】

【課題】　本発明は、複数のＷｅｂサーバで特定の利用者グループにアクセスを制限するために、利用者の手間を低減でき、Ｗｅｂサーバの運用管理の負担を少なくできる認証方法及びその装置を提供することを目的とする。

【解決手段】　クライアント端末２０から自装置のアクセス制限領域へのアクセス要求を受けた認証情報を持たない第１Ｗｅｂサーバ１０は、特定の利用者グループにアクセスを限定したアクセス制限領域を持ち認証情報を登録した第２Ｗｅｂサーバ３０に対し認証依頼を行い、第２Ｗｅｂサーバからの認証結果を受けた第１Ｗｅｂサーバは、認証結果に応じてクライアント端末からのアクセス制限領域のアクセスを行わせることにより、利用者の手間を低減でき、Ｗｅｂサーバの運用管理の負担を少なくすることが可能となる。

【選択図】　　図１

# 出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　　富士通株式会社